CLAIMS:

1. A method for assessing risk within an organization, comprising:

defining one or more zones, each of said one or more zones comprising an environment;

identifying one or more assets of said organization, each of said assets being located in a respective one of said zones;

conducting a respective impact assessment for each of said assets, each assessment comprising assessing the impact of the loss of said respective asset;

conducting for each of said zones a respective zone risk assessment, comprising assessing the risk level associated with placing a respective asset within said respective corresponding zone;

conducting for each asset a respective asset risk assessment, comprising assessing the risk level associated with said respective asset independent of the respective zone of said respective asset; and

assessing risk on the basis of at least said impact assessment, said zone risk assessments and said asset risk assessments.

2. A method as claimed in claim 1, including identifying one or more asset custodians, each comprising a custodian of a respective asset, and identifying one or more asset owners, each comprising an owner of a respective one or more of said assets.

3. A method as claimed in claim 2, wherein each of said custodians is an employee with care-taking responsibilities.

4. A method as claimed in claim 1, including maintaining a register of said assets.

5. A method as claimed in claim 4, wherein said register includes a respective owner of each of said assets.

6. A method as claimed in claim 1, including maintaining a register of said zones.

7. A method as claimed in claim 6, wherein said register includes a respective custodian of each of said zones.

8. A method as claimed in claim 1, wherein each of said assets is information related.

9. A method as claimed in claim 2, wherein each of said assets is information related, and each of said asset custodians is an information custodian, each comprising a custodian of a respective information storage device within said organization.

10. A method as claimed in claim 9, including defining at least four types of custodians: 1) physical and environment custodians, 2) network custodians, 3) software engineering custodians, and 4) MIS support custodians.

11. A method as claimed in claim 2, wherein each of said respective zone assessments is conducted by the respective custodian of said respective zone.

12. A method as claimed in claim 2, wherein each of said respective asset assessments is conducted by the respective owner of said respective asset.

13. A method as claimed in claim 1, including regarding the loss of an asset as equivalent to the loss of a system of which said asset is a part.

14. A method as claimed in claim 1, including determining a measured risk for each asset, said measured risk for a

respective asset comprising the product of 1) an impact level determined in said impact assessment and 2) the maximum of an asset risk determined in said asset risk assessment and an asset risk determined in said zone risk assessment.

15. A method as claimed in claim 2, wherein none of said custodians is an owner.

16. An apparatus for assessing risk within an organization, comprising:

data input means for inputting asset information into a register of assets, each of said assets being an asset of said organization, each of said assets being located in a respective zone;

data storage for storing said register of assets, including for each of said assets said respective zone;

means for receiving or storing a respective zone risk assessment for each of said zones, said respective zone risk assessment comprising an assessment of the risk level associated with placing a respective asset within said respective corresponding zone;

means for receiving or storing a respective asset risk assessment for each asset, said respective asset risk assessment comprising an assessment of the risk level associated with said respective asset independent of the respective zone of said respective asset;

means for receiving or storing a respective impact assessment for each of said assets, each assessment comprising assessing the impact of the loss of said respective asset, and for assessing risk on the basis of at least said impact assessment, said zone risk assessments and said asset risk assessments to thereby form a risk assessment; and

output means for outputting said risk assessment.

17. An apparatus as claimed in claim 16, wherein said

apparatus is operable to associate with each of said assets an asset custodian, each comprising a custodian of a respective asset, and to associate with each of said assets at least one asset owner, each comprising an owner of a respective one or more of said assets.

18. An apparatus as claimed in claim 16, wherein said register of assets includes a respective owner of each of said assets.

19. An apparatus as claimed in claim 16, wherein said apparatus includes data storage for storing a register of said zones.

20. An apparatus as claimed in claim 19, wherein said zone register includes data for associating a respective custodian with each of said zones.

21. An apparatus as claimed in claim 16, wherein each of said assets is information related.

22. An apparatus as claimed in claim 16, wherein said apparatus is operable to treat the loss of an asset as equivalent to the loss of a system of which said asset is a part.

23. An apparatus as claimed in claim 16, wherein said apparatus is operable to determine a measured risk for each asset, said measured risk for a respective asset comprising the product of 1) an impact level determined in said impact assessment and 2) the maximum of an asset risk determined in said asset risk assessment and an asset risk determined in said zone risk assessment.

24. A risk management method, comprising:

assessing risk according to the method of any one of claims 1 to 15; and

managing said risk.

25. A method as claimed in claim 24, wherein said managing of said risk comprises:

determining the distribution of the number of assets as a function of associated measured risk;

determining a maximum acceptable risk level; and

applying one or more controls if any of said assets exceeds said maximum acceptable risk level.

26. A method as claimed in claim 24, wherein said acceptable risk level comprises the lower of the highest available measured risk or 100%.